IN THE CLAIMS

1. (currently amended) An information processing system for distributing encrypted message data, said system comprising:

a receiving device, including:

holding ~~encryption processing~~ means for holding a key set that is specific to said receiving device and ~~that~~ which includes a portion of a plurality of node keys and a corresponding leaf key, the plurality of node keys being associated with ~~each~~ a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of leaves, the portion of the plurality of node keys being the node keys associated with the nodes disposed along ~~in~~ a particular path from ~~a top key~~ the root node of ~~a~~ the hierarchical tree structure to a particular one of the plurality of leaves~~f~~ ~~node~~ that is associated with said receiving device~~,~~ and with its corresponding ~~the hierarchical tree structure having a plurality of different devices as its leaves and having an associated~~ leaf key ~~for each device~~, and

encryption processing means for decrypting encrypted message data distributed to said receiving device by using ~~said~~ the key set; and

a distributing device, including:

message data generating means for generating ~~a renewal node key by which at least one of a plurality of node keys is renewed by said receiving device, the plurality of node keys and a plurality of leaf keys being respectively associated with a group constituted of nodes and leaves of the hierarchical tree structure, and for generating~~ an enabling key block (EKB) ~~within which said renewal node key is encrypted~~ using one ~~of~~ or more keys selected from the

group consisting of the portion of the plurality of node keys ~~or one of the plurality of~~ and the corresponding leaf key~~s~~, and

message data distributing means for distributing a storage medium storing first message data that includes data in which first content is encrypted with a content key, data in which the content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and storing second ~~to which other~~ message data that includes another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB) ~~is linked, the content encryption key being said renewal node key~~.

2. (currently amended) The information processing system according to claim 1, wherein said encryption processing means ~~in~~ of said receiving device obtains ~~said~~ a renewal node key by decrypting the ~~processing of said~~ enabling key block (EKB) ~~and executing decrypting of said encrypted message data by the renewal node key obtained~~.

3. (cancelled)

4. (currently amended) The information processing system according to claim 1, wherein ~~said~~ at least one of the first message data and the second message data includes an authentication key used in ~~the~~ authentication processing.

5. (currently amended) The information processing system according to claim 1, wherein ~~said~~ at least one of the first message data and the second message data includes a key for generating an integrity check value (ICV) of ~~the~~ its content.

6. (currently amended) The information processing system according to claim 1, wherein ~~said~~ at least one of the first

message data and the second message data includes a program code.

7. (cancelled)

8. (currently amended) The information processing system according to claim 1, wherein said message data distributing means and said receiving device ~~respectively~~ each include ~~have an~~ associated authentication processing means for executing authentication processing, and a distribution of said message data is performed on the condition that the authentication processing between said message data distributing means and said receiving device has been completed.

9. (currently amended) The information processing system according to claim 1, wherein ~~there exists a different~~ an intermediate device is disposed between said message data distributing means and said receiving device, and said message data distributing means generates and distributes ~~an~~ enabling key block (EKB) data and encrypted first and second message data that can be decrypted only in target devices targeted for distributing said message data.

10. (currently amended) The information processing system according to claim 1, wherein ~~said~~ the hierarch~~y~~ical tree structure includes a category group ~~constituted as a group, with one node as a top node, containing~~ that includes only the nodes and leaves which are ~~connected at~~ subordinate to a further one of the plurality of ~~of said top~~ nodes;

wherein ~~said~~ the category group is associated with ~~constructed as~~ a set of devices that belong to a category defined ~~solely~~ by a kind of ~~a~~ device, a kind of a service or a kind of a managing means.

11. (currently amended) The information processing system according to claim 10, wherein ~~said~~ the category group further includes one or more sub-category groups in the ~~lower stage of said~~ hierarch~~y~~ical tree structure;

wherein ~~said~~ the sub-category group is associated with ~~constructed as~~ a sub-set of ~~groups~~ devices that belong to a category defined ~~solely~~ by another ~~a~~ kind of ~~a~~ device, ~~a~~ kind of a service, or ~~a~~ kind of a managing means.

12. (currently amended) An information processing method for distributing encrypted message data, said method comprising: ~~a message data generating step of~~

generating ~~a renewal node key by which at least one of~~ a plurality of node keys ~~is renewed~~, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, ~~and a plurality of leaf keys being respectively associated with a group constituted of nodes and leaves connected at positions subordinate to a top node of~~ the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of ~~different devices as its~~ leaves, the plurality of leaves being associated with a plurality of leaf keys and with a plurality of devices whereby a given one of the plurality of leaves is associated with a specific one of the plurality of leaf keys and with a particular one of the plurality of devices; ~~and~~

generating an enabling key block (EKB) ~~within which said renewal node key is encrypted~~ using one ~~of~~ or more keys selected from the group consisting of the plurality of node keys ~~or one of~~ and the plurality of leaf keys; ~~a message data distributing step of~~

distributing a storage medium storing first message data that includes data in which first content is encrypted by a content key, data in which the content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in

which the content key encryption key is encrypted by the enabling key block (EKB), and ~~to which other~~ storing second message data that includes another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB) ~~is linked~~, the content key encryption key being ~~said~~ the renewal node key; and ~~a decrypting step of~~

decrypting, at a given one of the plurality of different devices, ~~said~~ the encrypted first message data using an associated key set that is specific to and stored in that device and using the data in which the content key encryption key is encrypted by the enabling key block (EKB), ~~each one of the plurality of different devices holding a different~~ the associated key set ~~formed of~~ including a specific portion of the plurality of node keys ~~specific to each~~ that are associated with the nodes ~~in~~ disposed along a particular path from the ~~top key~~ root node of ~~said~~ the hierarchical tree structure to a particular one of the plurality of leaves~~f~~ ~~node specific to~~ that is associated with that device and ~~a holding~~ including the leaf key ~~specific to~~ associated with that device so that the key set associated with a given one of the plurality of devices is different than the key set associated with another one of the plurality of devices.

13. (currently amended) The information processing method according to claim 12, wherein said decrypting ~~processing~~ step includes a renewal node key obtaining step of obtaining ~~said~~ a renewal node key by decrypting ~~processing of~~ the enabling key block (EKB)~~,~~, and a message data decrypting step for executing decryption of the encrypted first message data using the ~~by said~~ renewal node key.

14. (cancelled)

15. (currently amended) The information processing method according to claim 12, wherein ~~said~~ at least one of the first message data and the second message data includes an authentication key used in the authentication processing.

16. (currently amended) The information processing method according to claim 12, wherein ~~said~~ at least one of the first message data and the second message data includes a key ~~of~~ for generating an integrity check value (ICV) of its contents~~.~~

17. (currently amended) The information processing method according to claim 12, wherein ~~said~~ at least one of the first message data and the second message data includes a program code.

18. (cancelled)

19. (currently amended) The information processing method according to claim 12, further comprising an authentication processing step for executing authentication processing, and

wherein ~~said distribution of~~ said message data distributing step is performed on the condition that said authentication processing step has been completed.

20. (currently amended) The information processing method according to claim 12, wherein said message data distributing step generates and distributes ~~an~~ enabling key block (EKB) data and ~~an~~ encrypted first and second message data that can be decrypted only in a target device targeted for receiving said message data.

21. (currently amended) An information recording medium having stored therein data, said data comprising: ~~a renewal node key by which at least one of~~

a plurality of node keys ~~is renewed~~, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, ~~and a plurality of leaf keys being respectively associated~~

~~with a group constituted of nodes and leaves connected at positions subordinate to the top node of~~ the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of ~~different devices as its~~ leaves, the plurality of leaves being associated with a plurality of leaf keys and with a plurality of devices whereby a given one of the plurality of leaves is associated with a specific one of the plurality of leaf keys and with a particular one of the plurality of devices;

an enabling key block (EKB) ~~within which said renewal node key~~ which is encrypted using one ~~of~~ or more keys selected from the group consisting of the plurality of node keys ~~or one of~~ and the plurality of leaf keys; ~~and~~

first ~~a~~ message data that includes data in which first content is encrypted with a content key, data in which the content key is encrypted by a content key encryption key, and a link to a location on said information recording medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB); and

second ~~to which other~~ message data that includes another link to the location on said information recording medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB) ~~is linked, the content encryption key being said renewal node key~~.

22. (cancelled)

23. (cancelled)

24. (currently amended) The information recording medium according to claim 21 wherein said information recording medium stores an integrity check value (ICV) of at least one of the first content and the second contents~~,~~.

25. (currently amended) A ~~program providing~~ computer-readable medium for ~~providing a computer program~~ storing instructions for carrying out a method of decrypting encrypted content, said method comprising:

obtaining a storage medium storing first message data that includes data in which first content is encrypted by a content key, data in which the content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and storing second message data that includes another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB); ~~a renewal node key obtaining step of~~

obtaining an ~~renewal node key by linking to enabling key block (EKB) data within which the renewal node key is encrypted and to which other content is linked, decrypting the~~ enabling key block (EKB) using at least one ~~of~~ or more keys selected from the group consisting of a plurality of node keys ~~or one of~~ and a plurality of leaf keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of a plurality of node keys is associated with a particular one of the plurality of nodes, ~~and~~ the plurality of leaf keys being ~~respectively~~ associated with a ~~group constituted~~ plurality of ~~nodes and~~ leaves whereby a given one of the plurality of leaf keys is associated with a specific one of the plurality of leaves, ~~connected at positions subordinate to a top node of~~ the plurality of nodes being arranged according to a hierarchical tree structure having a ~~plurality of different devices as its~~ root node and the plurality of leaves, at

least one of the plurality of node keys being renewable ~~by~~ using the renewal node key;

decrypting, using the enabling key block, the data in which the content key encryption key is encrypted; ~~a step of~~

decrypting, using ~~said renewal node~~ the content key encryption key, ~~to obtain a~~ the data in which content key is encrypted; and ~~a step of~~

decrypting ~~said~~ the at least one of the encrypted first content using ~~said~~ the content key.

26. (currently amended) An information processing method for distributing encrypted message data, said method comprising:

generating ~~a renewal node key by which at least one of~~ a plurality of node keys ~~is renewed~~, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, ~~and a plurality of leaf keys being respectively associated with a group constituted of nodes and leaves connected at positions subordinate to a top node of~~ the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of ~~different devices as its~~ leaves, the plurality of leaves being associated with a plurality of leaf keys and with a plurality of devices whereby a given one of the plurality of leaves is associated with a specific one of the plurality of leaf keys and with a particular one of the plurality of devices;

generating an enabling key block (EKB) ~~within which said renewal node key is encrypted~~ using one ~~of~~ or more keys selected from the group consisting of the plurality of node keys ~~or one of~~ and the plurality of leaf keys; and

generating a storage medium storing first message data that includes data in which first content is encrypted by a

content key, data in which the content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and ~~to which other~~ storing second message data that includes another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB) ~~is linked~~, ~~the content encryption key being said renewal node key,~~ to distribute the first message data and the second message data to a plurality of devices.

27. (cancelled)

28. (currently amended) The information processing method according to claim 26, wherein ~~said~~ at least one of the first message data and the second message data includes an authentication key used in ~~the~~ authentication processing.

29. (currently amended) The information processing method according to claim 26, wherein ~~said~~ at least one of the first message data and the second message data includes a key ~~of~~ for generating an integrity check value (ICV) of contents.

30. (cancelled)

31. (currently amended) An information processing method, comprising:

obtaining a storage medium storing first message data that includes data in which first content is encrypted by a content key, data in which the content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and storing second message data that includes another link to the location on the storage medium wherein the data is stored in which the content key encryption key

is encrypted by the enabling key block (EKB); ~~a renewal node key obtaining step of~~

obtaining ~~a renewal node key by linking to enabling key block (EKB) data within which the renewal node key is encrypted and to which various contents are linked,~~ ~~decrypting~~ the enabling key block (EKB) using at least one ~~of~~ or more keys selected from the group consisting of a plurality of node keys ~~or one of~~ and a plurality of leaf keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of a plurality of node keys is associated with a particular one of the plurality of nodes, ~~and~~ the plurality of leaf keys being ~~respectively~~ associated with a ~~group constituted~~ plurality of ~~nodes and~~ leaves whereby a given one of the plurality of leaf keys is associated with a specific one of the plurality of leaves, ~~connected at positions subordinate to a top node of~~ the plurality of nodes being arranged according to a hierarchical tree structure having a ~~plurality of different devices as its~~ root node and the plurality of leaves, at least one of the plurality of node keys being renewable ~~by~~ using the renewal node key;

decrypting, using the enabling key block (EKB), the data in which the content key encryption key is encrypted; ~~a content key obtaining step of~~

decrypting, using ~~said renewal node~~ the content key encryption key, ~~to obtain a~~ the data in which content key is encrypted; and ~~an executing step of~~

decrypting ~~said~~ the encrypted first content using ~~said~~ the content key.

32. - 33. (cancelled)